

外部委託管理契約仕様（一般事項）

本委託作業の履行に当たり、下記各項に記載した事項について順守すること。

なお、下記各項において、受託作業の履行に当たり対象とならない事項については、東京逋信病院医療情報管理課（以下「主管課」という。）と協議の上、対象外とすることができる。

1 個人情報及び機密情報並びに預託情報の保全・安全管理措置の状況

1.1 受託者は、契約の履行に際して個人情報及び機密情報並びに預託情報（以下「個人情報等」という。）の紛失、漏えい、盗用、改ざん、目的外使用防止のために必要かつ適切な安全管理措置を講じること。

1.2 受託者は、作業員が本件業務遂行に際して知り得た個人情報等を第三者に漏らし、複製し、目的外に利用し、又は持ち出してはならないようにするため、作業員に対して個人情報等の秘密保持義務を遵守させるよう必要な措置を講じるとともに、必要かつ適切な監督を行うこと。

なお、委託期間終了後においても同様とする。

1.3 受託者は、本件受託業務の一部を第三者に再委託する場合は、事前に当社指定の様式「再委託承認申請書」、本業務に関わる業者（第三者）の当社指定の様式「適合証明書」、「安全管理状況確認票（個人情報等）」及び「安全管理状況確認票（機密情報）」を提出し、主管課の承認を得た上で受託した作業を実施すること。

なお、個人情報等に関する取扱いについては、受託者及び事前に主管課において承認された本業務に関わる業者間のみで取り扱うこと。

1.4 本件業務において個人情報等の紛失、漏えい、盗用等が発生又は発生するおそれのある場合、受託者は即時に原因等を究明し対応の上、併せて主管課に当該事由が発生した日時、場所等の内容及び対応状況を直ちに報告することとし、主管課が指示する場合は、その指示に従うこと。

1.5 受託者は、契約の履行に際して主管課から提供を受けた個人情報等については、委託作業終了後、直ちに個人情報等が記録されている媒体を主管課へ返却するとともに、主管課の承認を得た場合を除き、個人情報等を複製していない旨の証明書（様式適宜）を主管課へ提出しなければならない。

なお、受託者において主管課の承認を得て個人情報等をパソコン等に登録している場合は、委託作業終了後、受託者は直ちに一切のデータを消去し、データ消去に関する報告書（様式適宜）を主管課へ提出すること。

1.6 受託者は、個人情報等の安全管理に関する基本方針、個人情報等の取扱いに関する手続等を定めるとともに、本件受託業務にかかわるもの全員に対し遵守させること。

- 1.7 受託者は、個人情報等の取扱いに関し、取り扱いの総責任者及び取り扱う各部署の責任者を定めるとともに、個人情報等を取扱う各段階での従業員の役割と責任を社内取扱規定等に定め明確化しておくこと。
- 1.8 受託者は、個人情報等について権限を持たない者が見ることのないような体制を構築し、個人情報等を取扱う部屋等への入退室の管理を行うとともに、適切に保管する場所を確保すること。
- 1.9 受託者は、個人情報等の取扱いに関する点検・監査の手続等、安全管理措置の状況について確認する手続等を定めるとともに、定期又は随時に実施すること。
- 1.10 受託者は、個人情報等の外部委託に係る安全管理の手続等、再委託先に対する受託者の監督方法等を定めること。25
- 1.11 受託者は、再委託先の実態 25、個人情報等の取扱い状況、安全管理措置の状況について、再委託開始時及び終了時並びに定期的に報告を受けるとともに、定期又は随時に主管課へ報告し、当社が求めた場合は、速やかに再委託先に対し指導を行い改善を図ること。26
なお、再委託先の監督は、当社使用の「適合証明書」、「安全管理状況雄確認票（個人情報等）」及び「安全管理状況雄確認票（機密情報）」の内容を網羅した適宜な書式を用いて必要の都度、実施すること。
- 1.12 受託者は、個人情報等の授受を台帳等に記載し、授受や取扱履歴が確認できるように手続等を定めること。
- 1.13 受託者は、過去に情報の漏えい、き損等の事故を起こしていないこと。
なお、事故を起こしたことがある場合は、その後原因究明を行い、安全管理体制の構築を行っていること。
- 1.14 受託者は、本件業務で使用するパソコン、携帯電話等を東京逋信病院に持ち込む場合は、事前に東京逋信病院が指定する様式「情報機器等持込み機器使用計画書」を提出し、承認後に使用を開始すること。126
- 1.15 受託者は、パソコン等を使用する場合は、パソコン等のパスワードの設定及び運用を適切に行うとともに、起動時から有効なコンピューターウイルスチェックソフトウェアを稼働させること。
- 1.16 受託者は、責任者等の管理体制、個人情報等の管理の状況、安全管理措置の状況について、書面の提出など当社が求める監査方法に従い、速やかに監査に応じなければならない。
- 1.17 作業員が上記に違反することによって、東京逋信病院が損害を受けた場合、受託者がその損害をすべて補償しなければならない。

2 規程、手続、マニュアル等の整備等（委託先選定・業務遂行体制）

2.1 適切な業務遂行体制の整備

2.1.1 受託者は、本件受託業務の遂行に必要な事項について規程、手続、マニュアル等を定め、また必要に応じて見直しを行うこと。10

なお、規程、手続、マニュアル等は、事故を防止するための手順、事故発生時の報告方法等についても定め、リスク管理上の観点から十分なレベルであること。

2.1.2 受託者は、作業員に対し規程、手続、マニュアル等を遵守等するよう徹底を行うこと。11

2.2 業務履行の事務フロー

当該委託業務が、法令等に基づく義務の履行を含んでいる場合は、当該委託業務の業務フローは、当社自身が行った場合に課される法令上の義務の履行に支障が生じないフローであること。（対象の場合に適用する。）12

2.3 情報管理体制

2.3.1 情報管理ルール（情報の取扱いを含む業務の場合）

委託先において、委託業務に関する情報管理ルール（セキュリティーポリシー等）が制定され、遵守されていること。13

2.3.2 その他委託業務終了時の対応等

委託先に貸与した重要書類・ファイル・重要物（鍵・カード等）、資材、文書等、若しくはその複製物を業務終了時に委託元である当方に速やかに返却される体制を整備すること。（情報の取扱いを含む業務の場合）委託元情報資産について返却すること。または、データが消去されたことを確認できること。14

2.3.3 苦情相談への対応

委託業務に関し顧客から委託先へ苦情・要望・意見等が申し立てられた場合の苦情相談体制が整備され、また適切に対応できること。（対象の場合に適用する。）15

3 監査、報告、モニタリング体制

3.1 管理体制（立ち入り調査等検証の実施等）

定期的又は必要に応じて、事務処理の適切性の検証等を目的とした立ち入り調査・監査を実施できること。16

3.2 報告体制

3.2.1 業務に関する適切な定期報告ルール（方法・形式・報告事項等）を規定していること。17

3.2.2 業務に関する適切な都度報告ルール（方法・形式・報告事項等）を規定していること。18

4 業務管理体制

4.1 法令順守

4.1.1 当社の業務に従事する労働者に対し、公益通報者保護法に係る通報窓口について当社指定の周知文を受領したことを確認の上、当該周知文を用いて周知に努めること。19

4.1.2 受託者が、下請法の適用となる場合、それらの義務が守られ、禁止行為を行わないこと。（対象となる場合に適用とする。） 20

4.1.3 受託者は、本件受託業務を支障なく履行するために必要な事項について本件業務にあたる責任者の責任において作業員に対し業務指示、教育、指導等を行うこと。

なお、主管課は、受託業務を支障なく履行するために必要な事項について責任者に連絡し、責任者は結果責任及び誠意を持って対応、改善等を行うこと。 21

4.2 救急対応策の策定

受託者は、不測の事態による緊急対応が必要な場合を想定して、受託作業の継続履行に必要なコンティンジェンシープラン等を策定すること。 23

4.3 再委託先管理（委託先における再委託をする場合）

4.3.1 受託者は、個人情報等の外部委託に係る安全管理の手続等、再委託先に対する受託者の監督方法等を定めること。 25

4.3.2 受託者は、再委託先の実態 25、個人情報等の取扱い状況、安全管理措置の状況について、再委託開始時及び終了時並びに定期的に報告を受けるとともに、定期又は随時に主管課へ報告し、当社が求めた場合は、速やかに再委託先に対し指導を行い改善を図ること。 26

4.3.3 再委託先の監督は、当社使用の「適合証明書」、「安全管理状況雄確認票（個人情報等）」及び「安全管理状況雄確認票（機密情報）」の内容を網羅した適宜な書式を用いて必要の都度、実施すること。

また、個人情報又は顧客情報を取り扱う再委託先以降全ての委託先についても、委託先から定期的に報告（再委託開始時及び終了時を含む。）を行うこと。 27

4.3.4 業務委託内容

委託内容の不履行により、当院が高額な損害を被った損害賠償を履行するため、必要と認められる場合は、受託者の責任において相応の保険に加入するなどの備えを行うこと。 28

5 サイバーセキュリティ対策

5.1 体制

サイバーセキュリティについての部署ごとの役割（委託元への報告体制を含む）・責任が明確化されていること。 1

5.2 経営陣の関与

サイバーセキュリティについて経営陣が積極的に関与した上で、サイバー攻撃への対策措置に取り組むこと。2

5.3 監査

サイバーセキュリティに関する内部監査または外部監査を実施すること。3

5.4 リスクの認識

サイバーセキュリティの観点から、委託上実施する作業や環境にリスクがあるかないかを常に見直し対応すること。4

5.5 情報の収集

サイバーセキュリティに関する脅威や脆弱性等に関する情報を収集し、速やかに対応する体制であること。5

5.6 教育・周知

従業員に対し、サイバーセキュリティについての教育・周知を実施すること。6

6 サイバーセキュリティの対応

6.1 社外からのメールが受信できる端末を使用する場合（委託元が委託する機密情報等を保有するシステムにアクセス可能なメール利用端末も含む）

6.1.1 不審なメールの検知・遮断

通信を監視し、不審なメール等を検知・遮断する機能を整備すること。113

6.1.2 被害発生時の対処

標的型攻撃メールによる被害発生時の対処フローを整備し対処すること。114

6.1.3 電子メールの運用方針

電子メールの運用にあたっては、信頼性、安全性を確保するため、その運用方針が明確にすること。115

6.1.4 電子メール送受信、ホームページ閲覧等の不正使用防止

業務目的以外の電子メールの送受信、ホームページの閲覧等に対処するため、不正使用防止対策を講じること。

※ 本システムに接続する受託者の端末では、原則、電子メールの送受信や HP 閲覧等を行わないこと。

なお、やむを得ず行う場合は、メールフィルタリング等を導入し、不適切な情報の送受信を防止する、ホワイトリスト方式により、接続先を制御するなど、電子メール送受信、ホームページ閲覧等の不正使用防止対策を講じること。116

6.2 インターネットに接続するシステムを使用する場合

6.2.1 不審な通信の検知・遮断

通信を監視し、不審な通信の検知・遮断する機器等が整備すること。117

6.2.2 セキュリティ診断

新たなシステムによるサービス開始前に、セキュリティ診断を実施すること。既存システムについては、定期的にセキュリティ診断を実施すること。118

6.2.3 被害発生時の対処

不正アクセス等による被害発生時の対処フローが整備されており、対処できること。119

6.2.4 リソース共有時の攻撃影響

クラウドサービス契約のように、他社とリソースを共有する場合、他社のシステムへのサイバー攻撃が、当該システムに与えるリスクを認識すること。120

6.2.5 外部ネットワークからの不正アクセス防止

不正アクセスによるコンピュータシステムへの侵入を防ぐため、外部からアクセス可能な通信経路、通信関連機器等は最小限とし、不必要な機器を接続していないこと。121

7 その他

7.1 本仕様書に基づく契約締結後、保守体制を一覧にした表を主管課に提出すること。

なお、内容に変更が生じた場合は、速やかに現行化されたものを主管課に提出すること。

7.2 当社の各種データを取り扱う業務を受託する場合は、別添の「データ保護・管理要領」に必要事項を記載し主管課へ提出すること。提出の可否は主管課に確認すること。124

7.3 当院の情報資産を保管（設置）しているセキュリティ区画に対し、受託者は、当社保有外のパソコンやスマートフォン等の情報機器の持ち込み及び使用を禁止する。当院のセキュリティ区画については主管課に確認すること。125

7.4 当院の保護すべき情報資産がないと判断した特定場所へ、受託者が情報機器を持ち込む場合は、受託者に情報機器の持込みの届を提出すること。また、持ち込んだ情報機器の使用条件を明記させること。特定場所については主管課に確認すること。126

7.5 受託者は、受託業務に関わるもの全員（再委託等の場合の再委託先等を含む。）に対し院内の行動に関する倫理、道徳、社会常識、個人情報保護、情報セキュリティについて指導を行うこと。127

7.6 本仕様書に基づく受託作業において知り得た事項は、その内容を他に漏らしてはならない。

なお、本規定は、本契約期間終了後においても有効に存続する。

7.7 受託者は、本件受託に当たり東京逋信病院に対して虚偽の説明、意思表示、記載等を行ってはない。

- 7.8 本仕様書に基づく受託作業において、既存のシステム等の通常運用に支障を与えないよう配慮すること。
- 7.9 本仕様書に基づく受託作業において、予期せぬ事象が発生した場合は、速やかに主管課に報告するとともに、最善の対応を行うよう努めること。
- 7.10 当院の施設及び機器等を使用するに当たっては、善良なる管理者の注意義務を行使するとともに、万一、破損、き損及び亡失があった場合は、主管課へ報告の上、直ちに現状に修復等すること。
- 7.11 本仕様書に記載されていない事項で必要な項目又は詳細については、主管課（03-5214-7751）の指示に従うこと。

以上